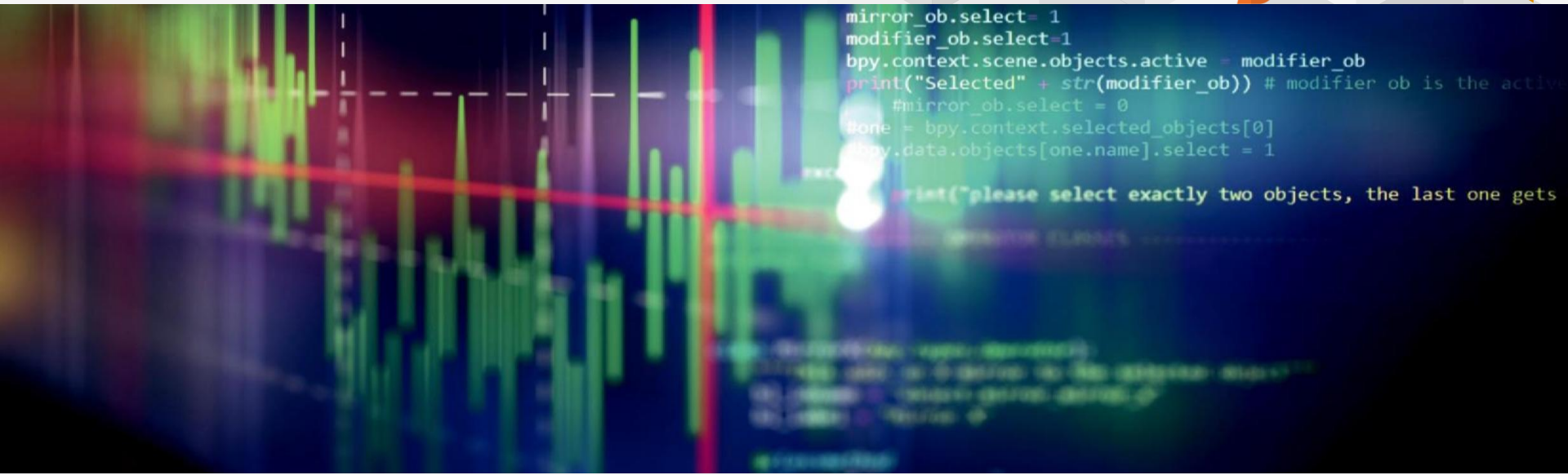
Đào tạo nhận thức Bảo mật thông tin cho CBNV

Theo tiêu chuẩn ISO/IEC 27001:2013

Nội dung đào tạo

01

Thông tin là gì?



01

Các dạng tồn tại của thông tin

Từng giây từng phút chúng ta đều tiếp xúc với thông tin ở các dạng tồn tại khác nhau

- Giấy in, bản viết tay
- Tệp, thư mục trên các thiết bị điện tử
- Hình ảnh, âm thanh, mùi hương…
- Cuộc hội thoại, tin nhắn, email
- Ý tưởng, kiến thức, kinh nghiệm, bằng cấp
- …

Thông tin là gì?

- Thông tin là một loại tài sản.
- Giống như tất cả các tài sản kinh doanh khác của công ty.
- Thông tin có giá trị đối với công ty phải được bảo vệ thích hợp.

- Theo ISO/IEC 27000:2018

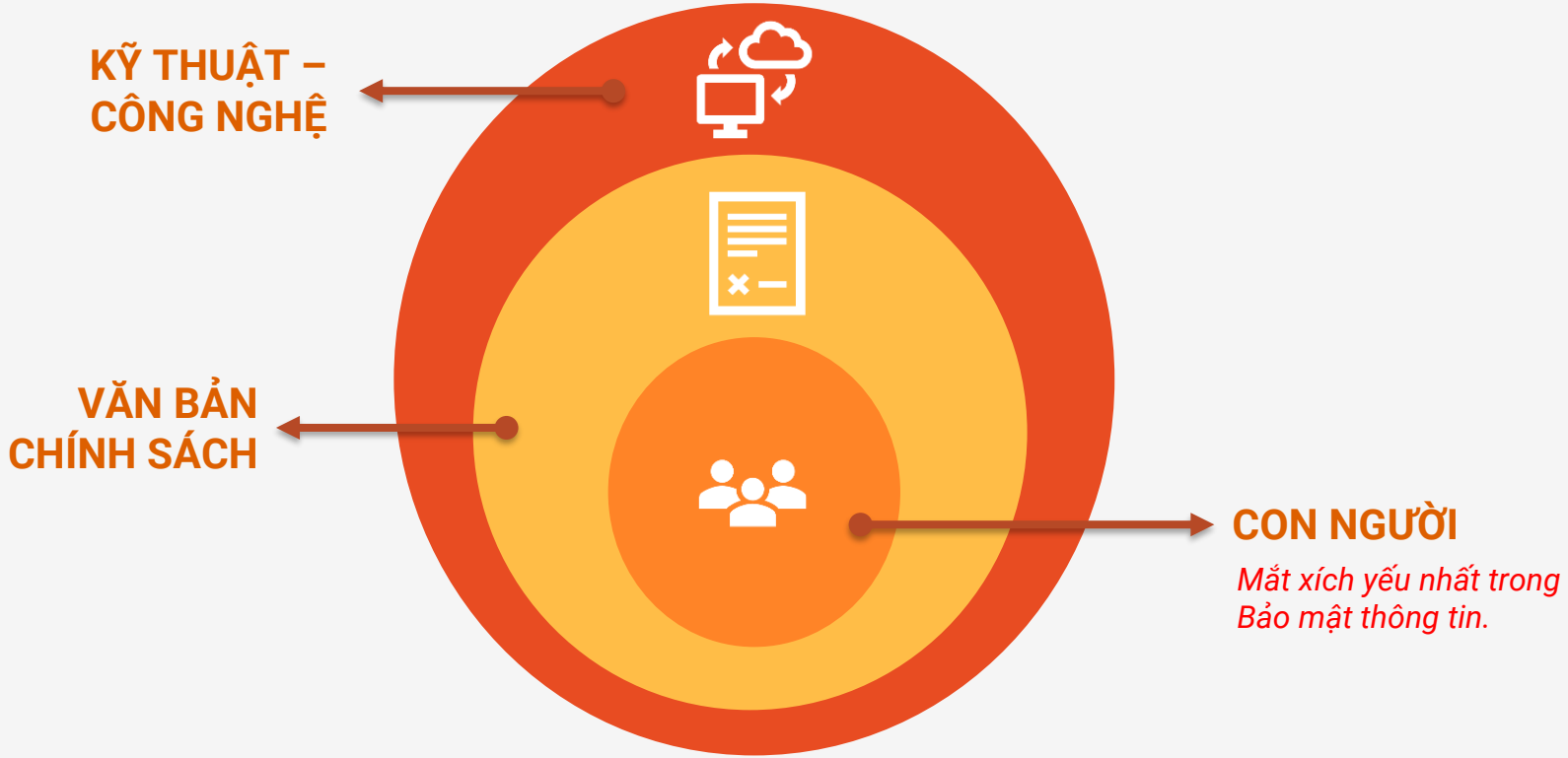
Bảo mật thông tin là gì?

Theo ISO/IEC 27000:2018, bảo mật thông tin (BMTT) là bảo vệ ba tính chất trọng yếu của một thông tin:

- Tính bí mật (Confidentiality)
- Tính toàn vẹn (Integrity)
- Tính sẵn sàng (Availability)

→ **Không phải lúc nào ba tính chất trên cũng quan trọng như nhau đối với một thông tin.**

Hệ thống Quản lý ATTT (ISMS)



Tài liệu BMTT tại FIS

Quy định chung về BMTT

- **“Quy định Quản trị BMTT”**

  (mã tài liệu QDQT-ISMS/FIS)

  – Chính sách ATTT
  – Phạm vi, cấu trúc Hệ thống Quản lý ATTT (ISMS) tại FIS
  – Quy định chung về BMTT tại FIS

- **“Quy định BMTT mức dự án”**

  (mã tài liệu 04-QD/ISMS/HDCV/FIS)

  – Đưa ra các Quy định BMTT dành cho dự án
  – Áp dụng trước, trong và sau khi triển khai thực hiện dự án

Chính sách ATTT

thuộc "Quy định Quản trị BMTT"

FIS đảm bảo:

- **Sự phù hợp** đối với các yêu cầu phát luật, chế định và các yêu cầu ràng buộc trong hợp đồng;
- **Tính tin cậy** của thông tin được đảm bảo;
- **Tính toàn vẹn** của thông tin được duy trì;
- **Tính sẵn sàng** của thông tin đối với các quy trình kinh doanh được duy trì;
- Thông tin được phân loại và các khu vực bảo mật được phân tách để **bảo vệ khỏi các sự truy cập** không được phép; **thiết lập, duy trì và thử nghiệm** kế hoạch đảm bảo hoạt động kinh doanh không bị gián đoạn;
- **Đào tạo BMTT** được thực hiện cho tất cả các cán bộ;
- **Vi phạm** về BMTT (có thật hoặc nghi ngờ) được thông báo cho Cán bộ phụ trách BMTT và được điều tra nghiêm túc;
- Bảo vệ các tài sản của tổ chức được truy cập bởi nhà cung cấp;
- Cam kết đảm bảo cải tiến liên tục hệ thống BMTT FIS.

Quy định BMTT cho cán bộ nhân viên

I. Thẻ nhân viên

- Đeo thẻ trong suốt thời gian làm việc tại Văn phòng FIS.
- **KHÔNG MƯỢN** và **CHO MƯỢN** thẻ.

II. Tài khoản truy cập

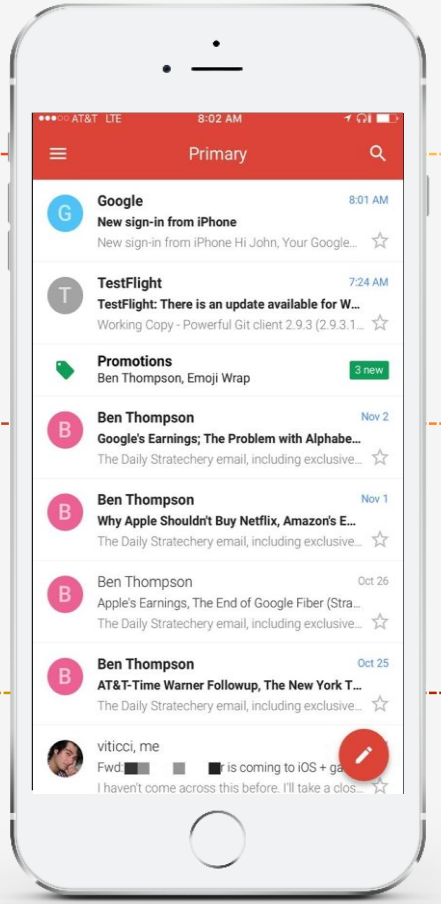
KHÔNG CHIA SẺ tài khoản truy cập các hệ thống thông tin của FIS cho bất kỳ ai, dưới bất kỳ hình thức nào.

III. Email FPT

Kiểm tra kỹ các trường To, CC, BCC, tệp đính kèm và nội dung email trước khi gửi

Cảnh giác với các email có dấu hiệu lừa đảo

Đặt mật khẩu cho file đính kèm chứa thông tin mật, gửi mật khẩu file đính kèm bằng phương thức khác.



KHÔNG sử dụng email công việc vào mục đích cá nhân (đăng ký mạng xã hội, mua sắm…)

KHÔNG chia sẻ mật khẩu email với bất kỳ ai dưới bất kỳ hình thức nào.

KHÔNG gửi các email spam, email quảng cáo cho các đối tượng trong và ngoài công ty.

IV. Bảo mật mật khẩu

Độ phức tạp

Bao gồm ít nhất 9 ký tự: ký tự chữ hoa, chữ thường, ký tự số và ký tự đặc biệt; Không chứa tên account hoặc một phần tên đầy đủ.

Lịch sử mật khẩu

Mật khẩu mới không trùng với 2 mật khẩu gần nhất trước đó.

Thời hạn mật khẩu

Thay đổi mật khẩu định kỳ mỗi 60 ngày (đối với Email FPT).

Khi nghi bị lộ mật khẩu

Thay đổi mật khẩu ngay lập tức khi nghi ngờ mật khẩu tài khoản đã bị lộ ra ngoài.

IV. Bảo mật mật khẩu

Dùng chung mật khẩu

KHÔNG dùng chung một mật khẩu cho nhiều tài khoản (tài khoản công việc, tài khoản cá nhân, mạng xã hội…)

Viết mật khẩu ra giấy

KHÔNG ghi chép mật khẩu ra giấy hoặc tệp văn bản.

“Nhớ” mật khẩu

KHÔNG sử dụng tính năng nhớ mật khẩu trên trình duyệt.

Chia sẻ mật khẩu

Tuyệt đối KHÔNG chia sẻ mật khẩu tài khoản truy cập của mình cho bất kỳ ai dưới bất kỳ hình thức nào.

IV. Bảo mật mật khẩu

Đặt mật khẩu cho file liệt kê password

Sử dụng các phần mềm ghi nhớ mật khẩu đáng tin cậy

Một số cách ghi nhớ mật khẩu an toàn

Trong trường hợp có quá nhiều tài khoản/mật khẩu cần ghi nhớ, chúng ta có thể sử dụng một số cách ghi nhớ mật khẩu an toàn như sau:

- Liệt kê các tài khoản/mật khẩu vào tệp văn bản và đặt mật khẩu cho tệp này.
- Sử dụng các phần mềm ghi nhớ mật khẩu đáng tin cậy.

V. Sử dụng Internet

Internet là môi trường lý tưởng để kẻ có ý đồ xấu tấn công những người dùng thiếu cảnh giác.

- Một số loại mã độc phổ biến
- Một số cách tấn công phổ biến
- Lưu ý khi sử dụng Internet

a. Một số loại mã độc phổ biến

Virus

Là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó tạo ra những tệp tin (file) bị nhiễm virus.

Trojan

Là chương trình độc hại ngụy trang như một cái gì đó được cho là lành tính.

Phần mềm gián điệp

Là loại phần mềm chuyên thu thập trái phép các thông tin của người dùng qua mạng Internet. Spyware thường được cài đặt bí mật kèm theo các phần mềm miễn phí.

Phần mềm tống tiền

Là loại mã độc sử dụng một hệ thống mật mã để mã hóa dữ liệu thuộc về một cá nhân và đòi tiền chuộc thì mới khôi phục lại.

Mã độc là một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và Internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức. Mã độc thực hiện các hành vi chuộc lợi cá nhân, kinh tế, chính trị hoặc đơn giản là để thỏa mãn ý tưởng và sở thích của người viết ra nó.

b. Một số kiểu tấn công phổ biến

Phishing

Lừa đảo (Phishing)

Là kiểu tấn công lừa đảo người dùng bằng cách tạo ra những thông điệp để thu hút sự tò mò của nhân nhằm bắt nạn nhân thực hiện một hành động như tải file, mở các tệp chứa virus, ấn vào đường link và nhập các thông tin liên quan. Những hành động này phục vụ cho mục đích của kẻ tấn công, có thể là: phát tán virus, lừa đảo thông tin, chiếm đoạt tài sản của nạn nhân…

b. Một số kiểu tấn công phổ biến

Malware

Tấn công bằng mã độc

Là kiểu tấn công mà kẻ có ý đồ xấu sẽ sử dụng mã độc (virus, trojan, phần mềm tống tiền, phần mềm gián điệp…) để thực hiện các hành động trái phép trên hệ thống/thiết bị của người dùng như thu thập thông tin, hiển thị các trang quảng cáo, lây nhiễm phát tán virus, mã hóa các tệp tin và đòi tiền chuộc…

Kiểu tấn công này thường được kết hợp với lừa đảo để dễ dàng đánh lừa người dùng cả tin.

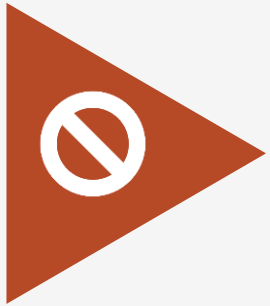
c. Lưu ý khi sử dụng Internet

Chặn quảng cáo

Cài đặt tính năng chặn quảng cáo (AdBlock) trên trình duyệt đang sử dụng.

Lừa đảo trên Internet

KHÔNG ấn vào các đường dẫn lạ, truy cập vào các trang web không rõ nguồn gốc hoặc làm theo các email có dấu hiệu lừa đảo.



Sử dụng trình duyệt an toàn

Sử dụng các trình duyệt web an toàn như Google Chrome, Firefox, Safari.

Chia sẻ thông tin mật

HẠN CHẾ chia sẻ các thông tin cá nhân trên Internet, KHÔNG sao chép, gửi các thông tin mật của công ty ra ngoài.

VI. Cài đặt và sử dụng phần mềm

Diệt virus

Cài đặt và sử dụng phần mềm diệt virus trên máy tính phục vụ công việc.

Dùng trình duyệt an toàn

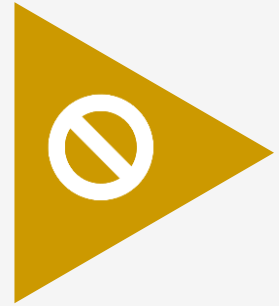
Sử dụng các trình duyệt web an toàn, đáng tin cậy: Google Chrome, Firefox, Safari,...

Tự động cập nhật

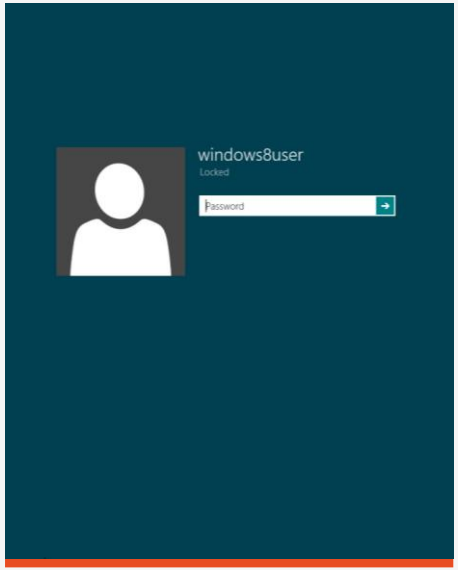
Đặt chế độ tự động cập nhật cho Hệ điều hành và phần mềm Anti-virus.

Dùng phần mềm crack

KHÔNG tải, cài đặt và sử dụng các phần mềm vi phạm bản quyền, phần mềm không rõ nguồn gốc.



VII. Chính sách “Màn sạch, Bàn sạch”



Màn sạch – Khóa/tắt máy khi rời khỏi chỗ ngồi

Bàn sạch – Dọn sạch bàn làm việc, cất tài liệu mật vào tủ có khóa khi rời khỏi chỗ ngồi

Hủy tài liệu mật trước khi vứt bỏ

VIII. BMTT tại các khu vực công cộng

Tránh để quên tài liệu, tài sản tại các khu vực công cộng không được giám sát: phòng họp, nhà ăn, khu vực máy in/scan/photocopy/fax, khu lễ tân…

IX. Lưu trữ dữ liệu

- Tất cả dữ liệu, thông tin bản mềm **dùng chung** trong bộ phận/nhóm/dự án và có mức độ quan trọng **Trung bình** trở lên phải được lưu trên **máy chủ chung** của FIS.
- Các máy chủ của FIS đều được sao lưu, phục hồi dữ liệu định kỳ để đảm bảo không bị mất mát, thất thoát dữ liệu.

IX. Lưu trữ dữ liệu

Dữ liệu dự án bản cứng

- Được lưu trong tập hồ sơ dự án
- Được quản lý bởi cán bộ quản lý hồ sơ của bộ phận/dự án.
- Được lưu trong tủ có khóa

Dữ liệu dự án bản mềm

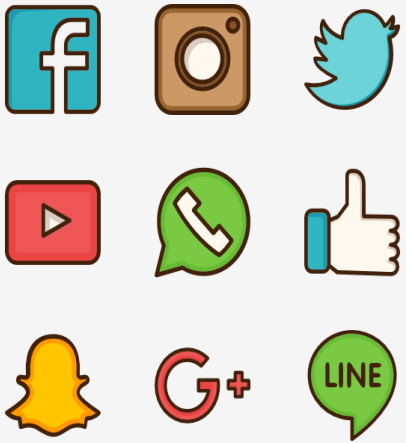
- Tài liệu sau khi được phê duyệt/bàn giao phải được chuyển lên thư mục lưu trữ chung (file server/SVN) của dự án.
- Source code phải được lưu trên SVN Server.

X. Bảo mật mạng

CẤM TUYỆT ĐỐI việc cắm các thiết bị thu phát sóng vào mạng của FIS.

→ Nếu vi phạm sẽ bị xử lý theo Quy chế Kỷ luật của Công ty.

XI. Sử dụng dịch vụ IT trên BA-Online



Sử dụng dịch vụ Internet
(Youtube, Facebook…)

Sử dụng tài nguyên nội bộ
(VPN, Teamview, FileServer…)

Đăng ký mang tài sản công ty
ra ngoài

XII. Bảo lãnh khách

- Đăng ký thông tin khách hàng, đối tác tại khu vực Lễ tân tầng 22 và làm thủ tục.
- Chỉ tiếp đón khách tại khu vực Lễ tân hoặc phòng họp.
- Không dẫn khách vào khu vực làm việc khi chưa đăng ký.

XIII. Đầu mối liên lạc

Thông báo ngay cho cán bộ ISMS khi nghi ngờ có sự cố BMTT xảy ra theo đầu mối:

- **FIS HN:**
  - **Ngô Thu Hồng** – HongNT53@fpt.com.vn
  - **Hotline IT HN: 2777**
- **FIS HCM:**
  - **Nguyễn Xuân Định** – DinhNX3@fpt.com.vn
  - **Hotline IT HCM: 80608**